Amendment to the Claims:

The following listing of claims replaces all previous versions and listings of claims:

1. (currently amended) An improved method of maintaining privacy for transactions employing a user device having a security module, wherein the improvement comprises the steps of:

receiving at a privacy certification authority computer a first set of signature values from the user device, the first set of signature values being generated by the user device using a first set of values obtained from an issuer to indicate that attestation was obtained from the issuer;

issuing a second set of values by the privacy certification authority computer to the user device, the second set of values based on a common value with the first set of signature values as an authority token;

receiving at a verification computer ~~a~~ the first set of signature values generated by the user device using ~~a~~ the first set of values obtained from ~~an~~ the issuer;

receiving at the verification computer a second set of signature values generated by the user device using ~~a~~ the second set of values obtained from ~~a~~ the privacy certification authority computer;

checking ~~at~~ by the verification computer the validity of the first set of signature values with a public key of the issuer;

checking ~~at~~ by the verification computer the validity of the second set of signature values with a public key of the privacy certification authority computer; ~~and~~

verifying a proof ~~at~~ by the verification computer that the first and second sets of signature values are based on the first and second sets of values that are obtained from ~~a~~ the common value, where the common value ~~that~~ is unique to the user device;

using a same base value by the privacy certification authority computer for a period of time

such that the privacy certification authority computer determines validity of the security module based on a frequency with which the security module has requested certification; and

issuing the second set of values by the privacy certification authority computer is performed in response to determining the validity of the security module

~~wherein the privacy certification authority computer uses a same base value for a sufficiently long period of time such that the privacy certification authority computer can determine a frequency with which the security module has requested certification, thereby allowing the privacy certification authority computer to identify whether the security module is a rogue security module~~.

2. (previously presented) The improved method according to claim 1, wherein the step of verifying comprises the step of:

verifying that a first value is derived from a base value included in the first set of -signature values, is identical with a second value that is obtained from the base value, and is included in the second set of signature values.

3. (canceled)

4. (previously presented) The improved method according to claim 2, wherein the base value is different each time the method is applied.

5. (currently amended) The improved method according to claim 1, wherein the common value is obtained from an endorsement key that is ~~related~~ allocated to the security module from the public key of the issuer.

6-20. (canceled)

21. (previously presented) The improved method of claim 1, wherein the common value is not forwarded to the security module in the user device.

22. (previously presented) The improved method of claim 1, wherein the privacy certification authority computer does not learn any useful information about the common value.

23. (previously presented) The improved method of claim 1, wherein the user device can use the second set of values only once and only with a given verifier.

24. (currently amended) A computer program product tangibly embodying computer readable instructions which when executed by an entity comprising a verification computer and a privacy certification authority computer causes the entity ~~the computer~~ to implement the steps of: ~~the improved method of claim 1~~

receiving at the privacy certification authority computer a first set of signature values from a user device having a security module, the first set of signature values being generated by the user device using a first set of values obtained from an issuer to indicate that attestation was obtained from the issuer;

issuing a second set of values by the privacy certification authority computer to the user device, the second set of values based on a common value with the first set of signature values as an authority token;

receiving at the verification computer the first set of signature values generated by the user device using the first set of values obtained from the issuer;

receiving at the verification computer a second set of signature values generated by the user device using the second set of values obtained from the privacy certification authority computer;

checking by the verification computer the validity of the first set of signature values with a public key of the issuer;

checking by the verification computer the validity of the second set of signature values with a public key of the privacy certification authority computer;

verifying a proof by the verification computer that the first and second sets of signature values are based on the first and second sets of values that are obtained from the common value, where the common value is unique to the user device;

using a same base value by the privacy certification authority computer for a period of time such that the privacy certification authority computer determines validity of the security module based on a frequency with which the security module has requested certification; and

issuing the second set of values by the privacy certification authority computer is performed in response to determining the validity of the security module.

DO NOT ENTER